Symantec Enterprise Firewalls

From the Internet

Thomas Jerry Scott

Symantec Firewalls

- Symantec offers a whole line of firewalls
- The Symantec Enterprise Firewall, which emerged from the older RAPTOR product
    - We are using this version in our class
- The 5400 Series of high end, integrated firewall offices for the enterprise
- The 100/200/200R series of appliance firewalls for the remote or small office

Symantec 5400 Series

- Symantec Gateway Security 5400 Series is a next-generation firewall appliance that integrates full packet inspection firewall technology with intrusion prevention intelligence at the gateway between the Internet and corporate network or between network segments.
- The solution leverages tightly integrated, industry-leading technologies to control and validate data packets as they pass through the gateway.

5400 Series Appliances - 2

- ***First,*** the firewall allows administrators to set granular policies for complete control of information entering and leaving the network
  - It performs deep packet inspection that drops and logs bad packets.
  - If a VPN session is active, the proxy-secured, VPN technology decrypts the packet and drops it into the data stream.
- ***Next,*** the firewall performs session checks at the circuit layer and once again, drops and logs bad packets.

- The integrated intrusion prevention and intrusion detection technologies block packets that contain threats
  - The IDS automatically notifies the the firewall of malicious sessions from specific IP addresses
- The firewall can then block specific sessions that contain threats or block specific IP addresses that continue to pose a threat.

Enterprise 5400 Firewalls - 3

- The firewall then opens and examines application layer protocol packets. These packets are checked to ensure conformity with the applicable RFCs and valid commands.
- Once again, bad packets are dropped and logged.
  - If the packets are HTTP based, content filtering technology compares the source IP against a list of prohibited Web sites. Prohibited content is dropped and logged.
- If the packets are HTTP, FTP, or SMTP protocol based, files and attachments are sent to the virus scanner
  - Actively blocks email messages by subject line text, file name attachment type, and message size.
  - If a virus is found, the file is either repaired or dropped.
  - All viruses are logged and a message is added to mail messages indicating that a virus was found and the attachment was deleted.
- If all of these checks are passed, the appliance allows the packet to enter or leave the network.
- This unique combination of security technologies helps stop viruses, malicious attacks, and blended threats at the network perimeter.

Symantec 4500 Series - 4

- **Security 5400 Series offers three high-performance models, all with an integrated high availability and load balancing option for maximum uptime.**

- **With its clustering and centralized management capabilities, Symantec Gateway Security provides robust and easily managed security for environments ranging from small offices to distributed networks with tens of thousands of nodes.**
- **Regardless of the network environment, the appliance delivers throughput that scales from 200 Mbps to more than 3.5 Gbps in clustered configurations.**

4500 Series Specifications

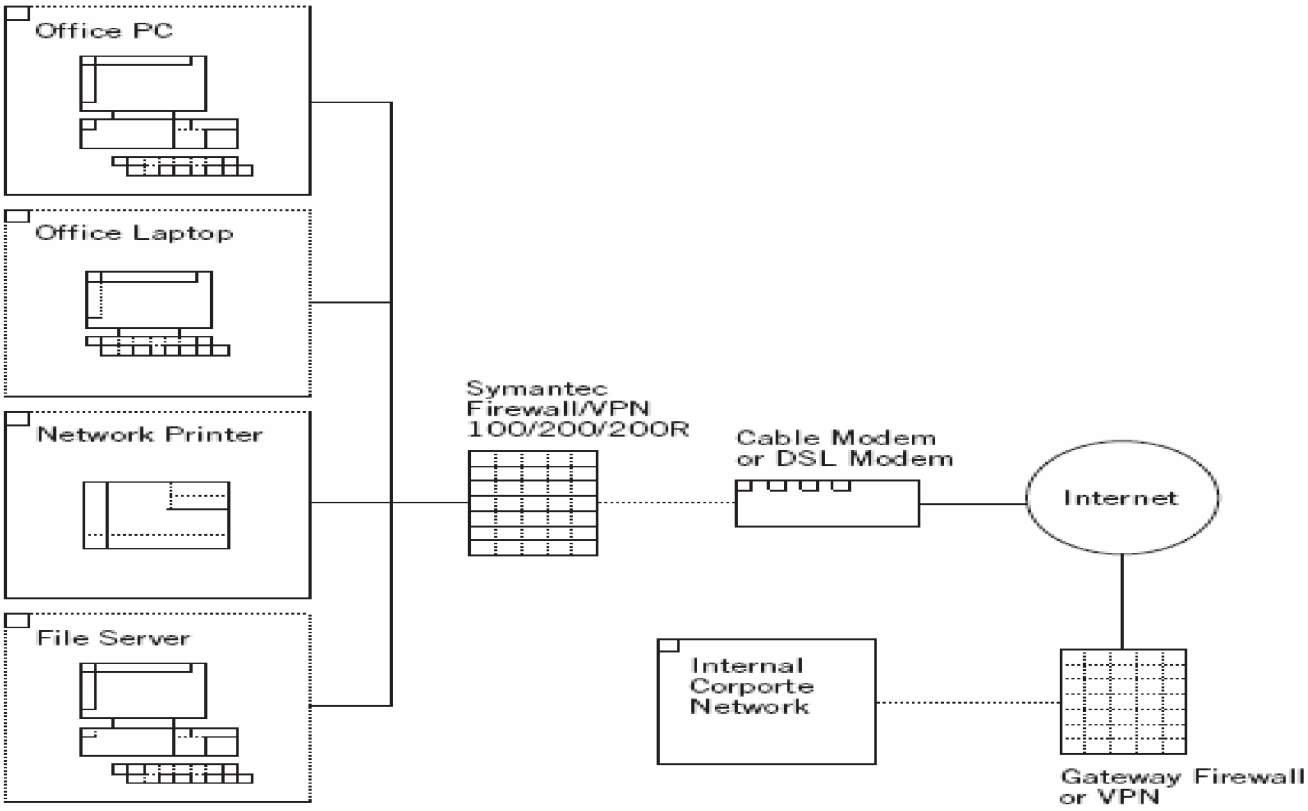
COMPARISON MODEL OF THE APPLIANCES

MODEL	5420	5440/5441	5460/5461
FEATURES			
Maximum Recommended Nodes	500	2500	4500
Stateful Thruput	200 Mbps	1.4 Gbps	1.8 Gbps
High-Availability Type	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)	A/A, A/P, LB (A/A - Active/Active; A/P - Active/Passive; LB - Load Balancing)
Maximum Cluster Size	8	8	8
Full Inspection	95 Mbps	680 Mbps	730 Mbps
VPN 3DES Encryption	90 Mbps	400 Mbps	600 Mbps
VPN AES Encryption	30 Mbps	80 Mbps	90 Mbps
Memory	512 MB	1 GB	2 GB
Disk	40 GB	80 GB	80 GB
Rack space	1U	2U	2U
Fast Ethernet NIC	6	0	0
Gigabit NIC	0	6 (Model 5441 - has 2 copper and 4 SX Multi-Mode fiber ports)	8 (Model 5461 has 2 copper and 6 SX Multi-Mode fiber ports)
Connections per second	5000	11300	15300
Concurrent Connections	64,000	190,000	200,000
PHYSICAL AND OPERATIONAL SPECIFICATIONS			
Operating Environment	5° C to 35° C (41° F to 95° F), 10% to 80% relative humidity, non-condensing	0° C to 40° C (32° F to 104° F), 10% to 80% relative humidity, non-condensing	0° C to 40° C (32° F to 104° F), 10% to 80% relative humidity, non-condensing
Non-Operating	-40° C to 65° C (-40° F to 149° F),	-40° C to 65° C (-40° F to 149° F),	-40° C to 65° C (-40° F to 149° F),
Environment	95% relative humidity, non-condensing	95% relative humidity, non-condensing	95% relative humidity, non-condensing
Operating Altitude	Up to 3000M (10,000 Ft)	Up to 3000M (10,000 Ft)	Up to 3000M (10,000 Ft)
Safety	UL 1950, EN 60950	UL 1950, EN 60950	UL 1950, EN 60950
Emissions	EN 55022 Class A, FCC Class A	EN 55022 Class A, FCC Class A	EN 55022 Class A, FCC Class A
Immunity	EN 55025	EN 55025	EN 55025
Height	4.45 cm (1.75 in)	8.9 cm (3.5 in)	8.9 cm (3.5 in)
Width	43.8 cm (17.25 in)	43.8 cm (17.25 in)	43.8 cm (17.25 in)
Depth	43.8 cm (17.25 in)	61 cm (24.0 in)	61 cm (24.0 in)
Weight	6.12 kg (13.6 lb)	9.59 kg (21.3 lb)	10.22 kg (22.7 lb)
Enclosure	Fits 19-inch Rack	Fits 19-inch Rack	Fits 19-inch Rack

Symantec Office Firewalls - 1

- These new small office firewall appliances form Symantec provide
  - Integrated Firewall Capability for Cable Modem and DSL
  - VPN Capability to connect to other small offices and a main corporate office
- Costs
  - 100 – Street price around $350
  - 200 – Street price around $550
  - 200r – Street price $800 - $900

Symantec Small Office Appliances



An example of how a Symantec Firewall/VPN appliance can be configured in a remote/small office environment.

Model 100/200/200R Compared

	MODEL 100	MODEL 200	MODEL 200R
Firewall	Yes	Yes	Yes
Gateway to Gateway VPN	Yes	Yes	Yes
Remote client to Gateway VPN	No	No	Yes
xDSL	Yes	Yes	Yes
Cable Modem	Yes	Yes	Yes
PPPoE	Yes	Yes	Yes
ISDN	Yes	Yes	Yes
T1	Yes	Yes	Yes
Recommended User Limit	25	40	40
	No License limitation	No License limitation	No License limitation
LAN Ports	4	8	8
WAN Ports	1	2	2
High Availability	Yes*	Yes*	Yes*
Load balancing	No	Yes	Yes

*With use of external modem and included Auto-Dial-Up Backup